

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC.,

Plaintiff,

v.

SKYRYSE, INC., ROBERT ALIN
PILKINGTON, MISOOK KIM, and DOES NOS.
1-50,

Defendants.

Case No.: No. 22-cv-00187

**PLAINTIFF'S OPPOSITION TO DEFENDANT SKYRYSE, INC.'S
MOTION TO COMPEL TRADE SECRET IDENTIFICATION**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. FACTUAL AND PROCEDURAL BACKGROUND.....	4
A. Moog’s Initial Filings Provide Substantial Information Regarding the Trade Secrets at Issue.....	4
B. Skyrise’s Consents to Expedited Discovery Regarding Moog’s Trade Secrets	5
C. Moog Provides Additional Available Information Regarding its Trade Secrets	6
D. Defendants Turnover Dozens of Electronic Devices and Tens of Thousands of Files to iDS.....	8
E. Moog Still Does Not Have Access to Skyrise’s Devices Turned Over to iDS	8
F. Skyrise Has Asserted its Trade Secret Identification Objections For Over Three Months	9
III. SKYRise’S MOTION SHOULD BE DENIED	10
A. Moog Has Sufficiently Identified its Trade Secrets at This Early Stage in Expedited Discovery	10
1. This Case is Functionally At the Pleading Stage	10
2. Moog Cannot Presently Identify Each File Misappropriated by Defendants	12
3. Moog Has Provided Available Information Despite Defendants’ Concealment of the Copied Files.....	14
4. Moog’s Trade Secrets are Available for Skyrise’s Inspection via IDS	15
5. Skyrise’s Cited Authority is Distinguishable.....	15
6. Former Skyrise Employees Kim and Pilkington Are the Best Sources of What Was Misappropriated	18
B. Skyrise’s Purported Burden and Volume Concerns are Unsubstantiated.....	19
1. Skyrise Consented to Expedited Discovery Regarding Moog’s Trade Secrets.....	19
1. Skyrise Has Not Substantiated any Purported Burden.....	19
C. Skyrise’s Requested Relief is Impracticable and Contrary to Law	20
1. Moog Has Properly Relied on Rule 33(d)	21

2. Moog is Not Required to Identify Each Line of Code That
Constitutes Non-Public Information22

IV. CONCLUSION.....24

TABLE OF AUTHORITIES**Page(s)****Federal Cases**

<i>Bytemark, Inc. v. Xerox Corp.</i> , No. 17 CIV. 1803 (PGG), 2022 WL 120980 (S.D.N.Y. Jan. 11, 2022).....	15
<i>Capricorn Mgmt. Sys., Inc. v. Gov't Emps. Ins. Co.</i> , 2016 WL 1370937 (E.D.N.Y. Apr. 6, 2016)	11
<i>Dardashtian v. Gitman</i> , No. 17-CV-4327, 2017 WL 6398718 (S.D.N.Y. Nov. 28, 2017).....	11
<i>DeRubeis v. Witten Techs., Inc.</i> , 244 F.R.D. 676 (N.D. Ga. 2007).....	13
<i>Harbor Software, Inc. v. Applied Sys., Inc.</i> , 887 F. Supp. 86 (S.D.N.Y. 1995)	23
<i>In Next Communications, Inc. v. Viber Media, Inc.</i> , 2016 WL 1275659 (S.D.N.Y. Mar. 30, 2016)	12
<i>Integ. Cash Mgmt. Servs., Inc. v. Digital Trans., Inc.</i> , 920 F.2d 171 (2d Cir.1990).....	22
<i>IntelliCAD Tech. Consortium v. Suzhou Gstarsoft Co.</i> , 508 F. Supp. 3d 790 (D. Or. 2020)	13
<i>Irth Sols., LLC v. Apex Data Sols. & Servs., LLC</i> , No. 18-CV-6884-FPG, 2019 WL 283831 (W.D.N.Y. Jan. 22, 2019).....	17
<i>John Wiley & Sons, Inc. v. Book Dog Books, LLC</i> , 298 F.R.D. 184 (S.D.N.Y. 2014)	20
<i>Liberty Power Corp., LLC v. Katz</i> , No. 10-CV-1938, 2011 WL 256216 (E.D.N.Y. Jan. 26, 2011)	11
<i>Lockheed Martin Corp. v. L-3 Commc'ns Corp.</i> , No. 1:05-CV-902-CAP, 2006 WL 8432941 (N.D. Ga. Oct. 27, 2006)	22
<i>Medtech Prod. Inc. v. Ranir, LLC</i> , 596 F. Supp. 2d 778 (S.D.N.Y. 2008).....	11, 13
<i>Next Commc'ns., Inc. v. Viber Media, Inc.</i> , No. 14-cv-8190 (RJS), 2017 WL 4402540 (S.D.N.Y. Sept. 30, 2017)	16

<i>Norbrook Lab'ys Ltd. v. G.C. Hanford Mfg. Co.</i> , 297 F. Supp. 2d 463 (N.D.N.Y. 2003), aff'd, 126 F. App'x 507 (2d Cir. 2005)	22
<i>Proofpoint, Inc. v. Vade Secure, Inc.</i> , No. 19-CV-04238-MMCM, 2020 WL 836724 (N.D. Cal. Feb. 20, 2020)	18
<i>Rensselaer Polytechnic Inst. v. Apple Inc.</i> , No. 1:13-CV-0633 DEP, 2014 WL 1871866 (N.D.N.Y. May 8, 2014)	21
<i>Sit-Up Ltd. v. IAC/InterActiveCorp.</i> , No. 05 CIV. 9292 (DLC), 2008 WL 463884 (S.D.N.Y. Feb. 20, 2008)	12, 16, 17
<i>Sorias v. Nat'l Cellular USA, Inc.</i> , 124 F. Supp. 3d 244 (E.D.N.Y. 2015)	11
<i>St. Jude Med. S.C., Inc. v. Janssen-Counotte</i> , 305 F.R.D. 630 (D. Or. 2015)	14
<i>T-Mobile USA, Inc. v. Huawei Device USA, Inc.</i> , 115 F. Supp. 3d 1184 (W.D. Wash. 2015)	14
<i>United States v. Nosal</i> , 844 F.3d 1024 (9th Cir. 2016)	22
<i>Xerox Corp. v. Int'l Bus. Machines Corp.</i> , 64 F.R.D. 367 (S.D.N.Y. 1974)	12
State Cases	
<i>MSCI Inc. v. Jacob</i> , 945 N.Y.S.2d 863 (Sup. Ct. 2012)	17
Rules	
Rule 12(b)	3, 11
Rule 33(d)	4, 20, 21, 22

I. INTRODUCTION

At the outset of this litigation, having been faced with a shocking and vast theft of its data, Moog prepared and served Skyryse with a complaint that provided a detailed narrative of the data taken, why it was critically valuable to Moog, and how it could be misused by Skyryse. In response, Skyryse stipulated to a temporary restraining order and expedited discovery to allow Moog to uncover the stolen trade secrets and to determine how it is has been used by Skyryse. Moog has spent the months since then attempting to obtain the discovery ordered by this Court and variously promised by Skyryse, but due to repeated obfuscation and delay by Skyryse, Moog still remains in the dark as to what Skyryse and its personnel have done with its data.

Four months into the case, Skyryse now claims that it “still does not know” a “single one” of the “trade secrets at issue.” This claim cannot be true given the following facts:

1. Its former employees Misook Kim and Alin Pilkington, who were fired months after this case was filed and the March 11 Order was entered, copied over 1.4 million files from Moog, deleted and obfuscated the copied files, and admittedly retained Moog’s non-public information when beginning employment at Skyryse. Kim and Pilkington knew exactly what they copied, and are intimately familiar with Moog’s trade secrets (setting aside the 18+ additional former Moog employees who worked alongside them).
2. Moog has provided to Skyryse the information available to it, including:
 - a. specifying that the trade secrets at issue as to the files copied by Kim include flight control source code and Software Engineering Process Group (“SEPG”) documents (as opposed to everything she copied).
 - b. providing logs containing:
 - i. a list of each of the 136,994 files copied by Misook Kim;
 - ii. a list of hash values for over 62,000 of those files at Skyryse’s request;

- iii. a folder log and timeline for the over 1.3 million files copied by Alin Pilkington; and
 - c. offering Skyryse 32 targeted search terms particular to Moog's source code.
3. Skyryse consented to expedited discovery regarding Moog's trade secrets at the outset of this case and has turned over to iDS, in response to the March 11 Order, 6 electronic devices and over 12,000 files containing presumptive Moog non-public data. Clearly Skyryse has an understanding of the trade secrets at issue in this case given its targeted productions made in response to the March 11 Order.

As this Court poignantly noted regarding Skyryse's prior request that Moog specifically identify each and every trade secret misappropriated by Defendants: "While Moog will have to identify them sufficiently in advance of the hearing to enable a proper defense, how can it be expected to do so now, when it does not yet know the full extent of what was taken?"

Skyryse's continued attempts to characterize itself as an innocent, small company being smothered by a larger competitor are confounding. Notwithstanding the lengthy struggles Moog has had in trying to obtain transparent information from Skyryse, it is undisputed that: 1) Moog non-public information correlated to the 1.4 million files Kim and Pilkington took upon leaving Moog and starting employment at Skyryse has been located at Skyryse in several locations; 2) Skyryse employees deleted relevant data and information related to this case after this lawsuit was filed; 3) Moog non-public information was used at Skyryse; and 4) at least 9 former Moog employees retained Moog non-public information upon beginning employment at Skyryse. This is just the information Moog has discovered without accessing the dozens of devices and millions of files turned over to iDS, and is likely just the tip of the iceberg.

The reality is that this case remains literally and functionally at the pleading stage. The case is not at issue. Skyrise does not dispute that Moog has met its specificity requirements at the pleading stage, and did not file any Rule 12(b) motion on such grounds. While Moog just received access to the iDS' review platform (which contain the key evidence regarding Skyrise's admitted possession of Moog data and deletion of data) on June 30, ***it still does not have access to any of the electronic devices Skyrise turned over because of Skyrise's delays in completing its privilege review and other logistical issues.*** Moog understands that it may need to further identify the trade secrets at issue in the case in advance of the Preliminary Injunction hearing, and has acknowledged as such during a hearing with the Court on June 1, 2022. However, Skyrise's request is premature. Skyrise's cited cases involving months or years of discovery and summary judgment do not apply here. The substantial available information that Moog has provided to date (well beyond its pleading obligations) is sufficient under the law.

Even if a different discovery standard applied, Moog would still only be required to identify the trade secrets misappropriated by Defendants, instead of any trade secrets that possibly relate to the subject matter of the lawsuit. Thus, as this Court acknowledged, Moog requires additional time to review the dozens of electronic devices and millions of files turned over to iDS to fully understand what was misappropriated by Defendants. Courts across the country recognize the need for trade secret plaintiffs to sufficiently conduct discovery before further specifying trade secrets, especially where it has been prevented from knowing exactly what was misappropriated.

While Skyrise claims overburden because of the scope of trade secrets discovery in this case, it can point the finger to its own former employees who copied over 1.4 million files and covered their tracks. It is improper for Skyrise to complain about burden or volume given the

undisputed conduct of its former employees. And, Skyryse cannot feign ignorance about the trade secrets at issue in this case when its own former employees know exactly what was copied and what happened to those files.¹ Skyryse has also not substantiated any overbreadth of volume concerns, such as through affidavits or declarations as required under the law. For example, Skyryse does not demonstrate the volume of its own flight control source code.

Skyryse now asks this Court to order Moog to provide a narrative response identifying with particularity every trade secret at issue in this case. This would require Moog to list each and every line of code from the tens of thousands of source code files that Moog has reason to believe were copied by Defendants. There is no legal or practical basis to compel such an order. Moog has properly relied upon Rule 33(d) at this stage and produced to iDS on June 1 the flight control programs, source code files, and other related trade secrets at issue. Skyryse has full access to Moog's source code and can conduct depositions about its specifics before its Opposition brief is due. There simply is no prejudice to Skyryse, and any purported prejudice is caused by the conduct of its current and former employees. Moog respectfully requests that this Court deny the Motion in full.

II. FACTUAL AND PROCEDURAL BACKGROUND

A. Moog's Initial Filings Provide Substantial Information Regarding the Trade Secrets at Issue

On March 8, 2022, Skyryse was served with Moog's Complaint and initial filings containing the following information regarding Moog's trade secrets:

¹ Skyryse should also not be heard to complain that now that Kim and Pilkington are former employees, they do not have access to them. Skyryse chose to terminate them both nearly two months after this action was filed and served. Therefore, Skyryse created this situation voluntarily for itself, and as such, is solely responsible for any issues it now has due to reduced access to Kim and Pilkington.

- i. specification of the two Moog-issued laptop and two external hard drive devices used by Kim to copy Moog's data (that Moog is aware of and has possession of). (Bagnald Dec. (ECF 4-18), ¶ 11) (*See generally* Pixley Dec. (ECF 4-28));
- ii. the dates, time, and manner in which Moog's data was copied by Ms. Kim on November 19, 2021 and December 15, 2021. (Bagnald Dec., ¶ 10) (Pixley Dec., ¶¶ 22-27);
- iii. a detailed breakdown by category of the 136,994 Moog files copied by Ms. Kim, including that 43,960 files constitute Moog source code. (Complaint, ¶ 115) (Bagnald Dec., ¶ 13) (Hunter Dec. (ECF 4-2), ¶ 43) (Schmidt Dec. (ECF 4-8), ¶ 19);
- iv. a detailed list of the commercial and military program classifications amongst the 136,994 files copied by Ms. Kim on November 19, 2021. (Complaint, ¶ 117) (Hunter Dec., ¶ 44) (Schmidt Dec., ¶ 20);
- v. a file log containing the file name, file path, external hard drive involved, encryption status, folder/hard drive name and location, file size, date and time of copying, and other unique identifiers *for each of the 136,994 files copied by Ms. Kim on November 19, 2021*. (the "File Log") (Bagnald Dec., Ex. A);
- vi. a detailed explanation regarding how the data copied by Ms. Kim on November 19, 2021 was intentionally altered, manipulated, and or deleted from Ms. Kim's Moog-issued laptop devices and/or the external hard drives used in the copying. (Complaint, ¶¶ 133-140) (*See generally* Pixley Dec.);
- vii. specification that the Moog trade secrets at issue in this case include flight control source code and Software Engineering Process Group ("SEPG") documents (as opposed to all data copied by Defendants). (Complaint, ¶¶ 39) (Hunter Dec., ¶¶ 28, 46).

During a discovery conference on June 1, the Court noted: "Mr. Hunter's declaration submitted in support of the motion for a preliminary injunction seems to identify with a fair level of specificity what the problem areas are." (ECF 170 (6/1/22 Tr.) at 5:10-13).

B. Skyryse's Consents to Expedited Discovery Regarding Moog's Trade Secrets

On March 11, 2022, Defendants stipulated to a temporary restraining order, rather than oppose Moog's motion for same, and the stipulation was entered as a Court order (the "March 11 Order"). (ECF 25, 28). Therein, Skyryse agreed to turn over all Moog non-public information in its possession, custody or control by April 1. Skyryse entered into the stipulation having full

notice of the allegations in the Complaint and the trade secrets at issue, and did not raise any challenge or objection to Moog's identification of trade secrets. In the March 11 Order, the Parties further agreed to meet and confer "to negotiate an agreed framework and schedule for reciprocal discovery relating to Plaintiff's Motion for Preliminary Injunction." (ECF 25, ¶ 10).

On March 17, 2022, the parties filed a stipulation regarding expedited discovery parameters and schedule. (ECF 33). Therein, Skyryse consented that: 1) Moog may propound 15 requests for production, 10 interrogatories, and 5 requests for admission; and 2) Moog may take a total of 5 depositions. (*Id.*). The expedited discovery stipulation also set forth, among other things, a detailed schedule for discovery, dispute resolution procedures, and protocols for conducting depositions. (*Id.*). Thus, Skyryse consented to extensive reciprocal discovery regarding Moog's trade secrets without raising any challenge to Moog's identification thereof. And, Skyryse never filed any pleading challenge to Moog's identification of trade secrets.

C. Moog Provides Additional Available Information Regarding its Trade Secrets

Moog's investigation continued after the filing of the Complaint in this action, and in a March 21, 2022 letter, Moog notified Defendants' counsel that it had found evidence of another series of downloads, this time by Pilkington. (Declaration of Rena Andoh ("Andoh Dec."), Ex. A). Moog explained that there was evidence that Pilkington had downloaded approximately 1.1 million files of Moog data from his Moog-issued laptop onto an external hard drive on the day Pilkington provided notice he was leaving Moog, and then subsequently downloaded another 130,000 files to another hard drive on his last day of employment by Moog. (*Id.*). Moog further explained that "efforts were taken to conceal this data transfer by Mr. Pilkington, which rendered it difficult for Moog not only to discover the theft, but to fully identify the breadth of it." (*Id.*).

On March 23, 2022, at Skyryse's request and as a supplement to the file log Moog had attached as an exhibit to the Complaint, Moog provided a log with MD5# values for

approximately 62,000 files from Kim's Moog-issued laptop that may correspond to certain of the 136,994 files that Kim copied from that laptop on November 19, 2021 (the "Hash Log"), and that this was all the hash information that Moog could generate in connection with the 136,994 files. (Andoh Dec., Ex. B). Moog further advised that the MD5# values are of limited probative value because, among other things, they were generated from files that could have been edited, altered, and/or manipulated by Kim or in the normal course of business after the copying occurred. (*Id.*).

On April 4, 2022, Moog provided Defendants' counsel with a log showing, among other things, folders copied by Pilkington and the timeline of his related conduct (the "Pilkington Folder Log"). (Andoh Dec. Ex. C at p. 4). Because Pilkington took efforts to conceal this data transfer, and because the hard drives used by Pilkington in these acts of copying are not available to Moog, Moog advised that it is unable to recover the specific file names and unique identifiers associated therein. (*Id.*).

In addition to the File Log Hash Log, and Folder Log, Moog has, at Skyryse's request, provided more targeted search terms to aid Skyryse in its search for Moog non-public information. Specifically, on April 12, Moog's counsel provided *a list of 32 highly-specific and targeted search terms* to help identify Moog non-public information, primarily source code. (Andoh Dec., Ex. D). Moog's cover e-mail noted that these search terms are not limiting or exhaustive, that they will not capture the likeliest misappropriating use of Moog's materials (such as Skyryse using Moog data as a reference, or copying/integrating portions of Moog data), and that Moog is providing "these search terms solely because [Skyryse's counsel] asked on Thursday's meet and confer for ways that Skyryse and its counsel can search for potentially relevant files on Skyryse's system and devices." (*Id.*). Thus, Moog has provided to date a wealth

of information regarding the over 1.4 million files copied by Kim and Pilkington, and will continue to provide additional information as it becomes available.

D. Defendants Turnover Dozens of Electronic Devices and Tens of Thousands of Files to iDS

Despite Skyryse's claim that it does know a single trade secret at issue in this case, pursuant to the March 11 Order it admits that it has turned over to iDS: 1) Kim's Skyryse-issued laptop; 2) Pilkington's two Skyryse-issued laptops; 3) 11,093 files from Pilkington's Skyryse-issued laptops that hit on the file names from the File Log; 4) a hard drive containing 568 non-human readable files; 5) a USB drive containing two source code repositories that hit on the 32 narrowly tailored search terms provided by Moog on April 12; 6) the Skyryse-issued laptop and USB drive of engineer Alex Wang who Skyryse admits deleted at least 44 relevant files after this lawsuit was filed; and 7) 12 of the 44 deleted files that were recoverable. (Mot. at pp. 14-15). Kim and Pilkington have turned over 23 electronic devices.

Skyryse represents that it has "collected and preserved millions of potentially relevant files in connection with this action." (ECF 156 at p. 1). Yet, it clearly has a specific understanding (due in large part to the File Log, Hash Log, Folder Log, and other information provided by Moog) of the trade secrets at issue in this case, given its targeted production of devices and data to iDS that all presumptively contain Moog information.

E. Moog Still Does Not Have Access to Skyryse's Devices Turned Over to iDS

Under Moog's Inspection Protocol which has been entered by the Court (ECF 96-02, 109), Skyryse's privilege review was supposed "to be complete such that Authorized Reviewers can commence inspection of these devices" by the date ordered by the Court, which was June 24 pursuant to the Parties' June 2 stipulation and order (ECF 137). While Skyryse did send logs to iDS for privileged materials to be excised on June 16 and June 27, the logs only pertained to

some but not all of the devices turned over to Skyryse. (Andoh Dec., Ex. E). Further, there are formatting and logistical issues with those logs, which iDS first asked Skyryse to correct on June 21. (*Id.*). Moog's team received inspection laptops and first obtained access to iDS' review platform on June 30. However, because of Skyryse's delays in completing privilege review and fixing other technical issues (in contravention of the June 2 stipulation and order), ***Moog still does not have any access to any of Skyryse's electronic devices, including the Skyryse-issued laptops for Kim and Pilkington.***

F. Skyryse Has Asserted its Trade Secret Identification Objections For Over Three Months

The timing of Skyryse's Motion is curious given that it has raised this issue to Moog and the Court repeatedly over the past three months. Skyryse first raised this purported objection in its April 1 letter where it falsely certified that it had complied with its obligations under the March 11 Order. (Andoh Dec., Ex. F). Skyryse raised this purported issue again in several written correspondence with Moog and filings with the Court, including but not limited to its May 11 Motion for Adoption of Forensic Protocol (ECF 99-1 at pp. 7-9), May 27 Opposition to Moog's Motion for Scheduling Orders (ECF 128 at pp. 8-10), and June 14 Opposition to Moog's Motion to Compel (ECF 156 at pp. 3, 6).

On May 25, 2022, Magistrate Judge McCarthy sent an e-mail to the parties, and regarding Skyryse's argument regarding Moog's purported failure to identify its trade secrets, noted: "While Moog will have to identify them sufficiently in advance of the hearing to enable a proper defense, how can it be expected to do so now, when it does not yet know the full extent of what was taken?" (Andoh Dec., Ex. G).

During a June 1 discovery conference, the Court reiterated this point: "it's unrealistic to expect Moog to identify all of its trade secrets when it doesn't know the full scope of what has

been taken.” (ECF 170 at 5:8-10). During the same hearing, Skyryse’s counsel agreed: “We understand the points that they’ve made that some files have changed, that some files are not static and that they may not know, at this point, with one 100 percent precision every file that has been taken.” (*Id.* at 20:9-13).

III. SKYRYSE’S MOTION SHOULD BE DENIED

A. Moog Has Sufficiently Identified its Trade Secrets at This Early Stage in Expedited Discovery

1. **This Case is Functionally At the Pleading Stage**

Skyryse argues that the pleading standard for trade secret identification is irrelevant and Moog’s discovery obligation to identify its alleged trade secrets is subject to a higher standard. Skyryse also claims that there is “no excuse for Moog’s failure to identify its alleged trade secrets . . . at this point after receiving extensive discovery from Defendants.” (Mot., p. 15). However, this misrepresents the state of discovery. Skyryse acknowledges that in response to the March 11 Order, it has turned over to iDS several electronic devices and tens of thousands of files to iDS. (*Id.*, pp. 14-15). But, what Skyryse does not inform the Court is that the Moog first obtained access to any device in iDS’s possession just a few days ago on June 30, ***and it currently has no access to any Skyryse electronic device due*** to Skyryse’s untimely completion of privilege review and other logistical issues. More time is needed for Moog’s counsel and experts to analyze the three dozen devices and potentially millions of files in iDS’s possession before ascertaining the extent of Defendants’ misappropriation, spoliation, and other conduct that has already been disclosed to the Court. Asking Moog to identify every single line of non-public source code that has been misappropriated when it does not yet have access to Skyryse’s devices turned over to iDS.

Given this procedural posture, this case is literally and functionally at the pleading stage. First, the case is not at issue and Defendants' Rule 12(b) motions to dismiss have not been adjudicated. Second, the parties just recently made initial document productions on June 2, and Skyryse's devices and files produced to iDS have still not been made available to Moog. Thus, the pleading requirements for trade secret claims are relevant to this dispute. And, Moog's trade secret descriptions and related information far exceed the particularity requirements applied by district courts in this circuit. *See, e.g., Capricorn Mgmt. Sys., Inc. v. Gov't Emps. Ins. Co.*, 2016 WL 1370937, at *3 (E.D.N.Y. Apr. 6, 2016) (claim that plaintiff's proprietary program "enhanced" fraud detection, enabled "customization and automation of the claims management process," monitored employee efficiency and detected fraudulent prescriptions was sufficient to identify trade secrets); *Medtech Prod. Inc. v. Ranir, LLC*, 596 F. Supp. 2d 778, 789 (S.D.N.Y. 2008) ("The Court recognizes that Medtech, for the most part, does not specify the particular trade secrets at issue in this case, but instead categorizes them generally as 'manufacturing cost details, drawings, test data, and other information about the design and manufacturing process for its dental protectors.' However, specificity as to the precise trade secrets misappropriated is not required in order for Medtech to defeat the present Motions to Dismiss."); *Sorias v. Nat'l Cellular USA, Inc.*, 124 F. Supp. 3d 244, 259 (E.D.N.Y. 2015) ("though general," complaint's identification of trade secrets as "data and designs of a specific phone charger with horizontally folding A/C prongs" was sufficient to give defendants fair notice of the claim); *Liberty Power Corp., LLC v. Katz*, No. 10-CV-1938, 2011 WL 256216, at *2 (E.D.N.Y. Jan. 26, 2011) (one of the trade secrets identified by the plaintiff was described as "specific contact information for individual contacts at Plaintiff's customers," and this was considered sufficient); *Dardashtian v. Gitman*, No. 17-CV-4327, 2017 WL 6398718, at *5 (S.D.N.Y. Nov. 28, 2017) (Court concluded

that a trade secret disclosure of “customer lists and addresses, vendor lists and addresses, computer software programs; computer pass codes and other protectable intellectual property and proprietary information” provided a “level of detail ... adequate for defendants to discern the trade secrets at issue.”); *In Next Communications, Inc. v. Viber Media, Inc.*, 2016 WL 1275659, at *4 (S.D.N.Y. Mar. 30, 2016) (complaint’s description of a “unique technique for routing calls, allowing for detailed traffic monitoring, reporting, and billing” was adequate to identify the claimed trade secret.).

2. Moog Cannot Presently Identify Each File Misappropriated by Defendants

Even if the pleading standard for trade secret identification was not applicable here (which it is), Skyrise misses a key point in its legal analysis. Moog is not required to simply identify any trade secret that relate to the subject matter of this case. Rather, and under the very authority cited by Skyrise, Moog’s trade secret identification requirements are limited to the trade secrets that *were misappropriated by Defendants*. See *Xerox Corp. v. Int’l Bus. Machines Corp.*, 64 F.R.D. 367 (S.D.N.Y. 1974) (ordering the plaintiff to “identify in detail all trade secrets and confidential information *alleged to have been misappropriated by IBM*”) (emphasis added); *Sit-Up Ltd. v. IAC/InterActiveCorp.*, No. 05 CIV. 9292 (DLC), 2008 WL 463884, at *11 (S.D.N.Y. Feb. 20, 2008) (holding the plaintiff’s burden includes describing the “alleged trade secret with adequate specificity to inform the defendants *what it is alleged to have misappropriated*.”).

Here, as this Court has acknowledged, Moog cannot presently identify with specificity each and every trade secret misappropriated by Defendants because of the data deletion and other obfuscation committed by Defendants. Thus, Moog will not be able to connect the dots and understand the full extent of what was taken until it has had an opportunity to completely evaluate the Skyrise’s devices and files turned over to iDS.

It is for this exact reasons that courts routinely allow a trade secret plaintiff the opportunity to conduct discovery before being required to identify its trade secrets with specificity, for a variety of reasons. These reasons are best summarized in *DeRubeis v. Witten Techs., Inc.*, 244 F.R.D. 676 (N.D. Ga. 2007):

“[C]ourts have identified at least three policies which support allowing the trade secret plaintiff to take discovery prior to identifying its claimed trade secrets. First, courts have highlighted a plaintiff’s broad right to discovery under the Federal Rules of Civil Procedure. . . . Second, the trade secret plaintiff, ***particularly if it is a company that has hundreds or thousands of trade secrets, may have no way of knowing what trade secrets have been misappropriated until it receives discovery on how the defendant is operating.*** . . . Finally, if the trade secret plaintiff is forced to identify the trade secrets at issue without knowing which of those secrets have been misappropriated, it is placed in somewhat of a ‘Catch-22’ because “[s]atisfying the requirement of detailed disclosure of the trade secrets without knowledge [of] what the defendant is doing can be very difficult. ***If the list is too general, it will encompass material that the defendant will be able to show cannot be trade secret. If instead it is too specific, it may miss what the defendant is doing.***” *Id.* at 680 (emphasis added).

Here, where the scope of Defendants’ misappropriation has placed tens of thousands of trade secrets at issue, Moog must conduct discovery to determine what was taken and how it has been used by Skyryse. Courts in similar circumstances have allowed discovery before specific trade secret identification. *See IntelliCAD Tech. Consortium v. Suzhou Gstarsoft Co.*, 508 F. Supp. 3d 790, 800 (D. Or. 2020) (denying motion to compel interrogatory responses, permitting the plaintiff to “inspect Gstar’s source code under appropriate conditions of confidentiality” and then determining “after a reasonable (but not too long) time, the ITC will need to provide more specific responses to Gstar’s interrogatories, ***although limited to the specific trade secrets that the ITC contends were misappropriated by Gstar*** (i.e., not all trade secrets owned by the ITC).”) (emphasis added); *Medtech Prod. Inc. v. Ranir, LLC*, 596 F. Supp. 2d 778, 819–20 (S.D.N.Y. 2008) (“I conclude that Medtech should be allowed limited discovery on the trade secret claim prior to being required to identify the precise trade secrets it is alleging were misappropriated.”);

This right to discovery is heightened where there are undisputed findings of deletion of data or other obfuscation of the nature and scope of the misappropriated data. *St. Jude Med. S.C., Inc. v. Janssen-Counotte*, 305 F.R.D. 630, 641 (D. Or. 2015) (the plaintiff was not required to identify its trade secrets with greater particularity before taking discovery, in part because “Plaintiff appears to have numerous trade secrets but...no way of knowing which trade secrets have been misappropriated until it receives discovery on how the defendant is operating.”); *T-Mobile USA, Inc. v. Huawei Device USA, Inc.*, 115 F. Supp. 3d 1184, 1193 (W.D. Wash. 2015) (Noting that “because it is the defendant who knows what it misappropriated, a plaintiff should not be compelled to divulge with specificity all of its possible trade secrets (especially not to a defendant who it believes has already misappropriated at least one of them) in order to proceed to discovery”);

Simply put, given the facts of this case, Skyryse’s motion is premature because Moog is entitled to fully review the voluminous data turned over to iDS to understand the full nature of Defendants’ misappropriation before further identifying its trade secrets at issue in this case.

3. Moog Has Provided Available Information Despite Defendants’ Concealment of the Copied Files

Notwithstanding the limited information available to Moog, Skyryse’s claim that it “does not know what trade secrets are at issue—not a single one” is simply not congruent with the record before this Court. For the 136,994 files copied by Kim, Moog has provided file names for each file, and provided hash values for over 62,000 of those files. For the over 1.3 million files copied by Pilkington, Moog is unable to identify the files given the deliberate obfuscation by Pilkington but has identified the folder paths copied by Pilkington. Moog has also provided to Skyryse a targeted list of 32 search terms unique to Moog source code.

Moog has gone above and beyond its initial identification requirements to provide Skyryse with the information available to it regarding the over 1.4 million files copied by Kim and Pilkington. Indeed, Skyryse’s Motion is silent on what additional information Moog could possibly provide at this stage in the case given the circumstances.

4. Moog’s Trade Secrets are Available for Skyryse’s Inspection via IDS

Skyryse’s broad-sweeping claims that Moog “refused to identify its trade secrets” or is taking a “shoot-first-aim-later” approach to this case are simply false. As Moog indicated in its supplemental interrogatory response, the trade secrets identified by Moog (including its flight control source code) are located on the devices that Moog has produced to iDS. Pursuant to the Inspection Protocol, Skyryse has full access to these devices and the files contained therein. Moog is not hiding anything or refusing to produce its trade secrets. *See Bytemark, Inc. v. Xerox Corp.*, No. 17 CIV. 1803 (PGG), 2022 WL 120980, at *5 (S.D.N.Y. Jan. 11, 2022) (where the plaintiff agreed to “identify its trade secrets immediately through production of all of the source code and confidential information in its possession,” the court held: “This case is in its very early stages. . . . At this stage of the litigation, Plaintiff is not required – as a prerequisite for obtaining relevant discovery from Defendants – to identify its trade secrets with the specificity that Defendants demand.”).

5. Skyryse’s Cited Authority is Distinguishable

Skyryse argues that the pleading standard is irrelevant and Moog’s discovery obligation to identify its alleged trade secrets is heightened. While this case remains functionally at the pleading stage for reasons set forth above, the cases cited by Skyryse on pages 11-12 of its Motion are distinguishable and show why its repeated demands for further trade secret identification are inappropriate at this stage in the case.

Next Commc'ns., Inc. v. Viber Media, Inc., No. 14-cv-8190 (RJS), 2017 WL 4402540 (S.D.N.Y. Sept. 30, 2017) is not applicable on its face because it involved adjudication of a motion for summary judgment ***which was filed two years after the lawsuit was filed and after the close of "Phase I" discovery.*** *Id.* at *2. The court granted summary judgment in favor of the defendant because "after more than two years of litigation, including several months of Phase I discovery in which the Court ordered Next to define its alleged trade secrets with the required particularity (Doc. No. 87), Next still has not done so." *Id.* at *6. This is nothing like the procedural posture of this case, where the case was filed four months ago, the parties are far from completing expedited discovery, and Moog still does not have access to the majority of the iDS data. Further, after months of discovery, the defendant in Viber Media defined its trade secrets as the "GSM-IP Mobile Network," "Secure Financial Network," and "HD Video Cloud Architecture" without any further specificity. *Id.* at *4. This pales in comparison to all of the specificity and information provided by Moog (i.e., the File Log, Hash Log, and Folder Log).

Similarly, *Sit-Up Ltd. v. IAC/InterActiveCorp.*, No. 05 CIV. 9292 (DLC), 2008 WL 463884 (S.D.N.Y. Feb. 20, 2008) involved a motion for summary judgment ***that was decided more than 27 months after the complaint was filed.*** Thus, the plaintiff had multiple years to conduct discovery to support its claims. Here, Moog still does not have access to any of Skyrise's electronic devices that most significantly relate to its misappropriation claims. The two circumstances are not the same. Finally, in *Sit-Up*, the plaintiff took the position that "it need not identify its alleged trade secrets with specificity." *Id.* at *11. Moog has never taken this position. Rather, and as acknowledged by this Court, "how can it be expected to do so now, when it does not yet know the full extent of what was taken?"

MSCI Inc. v. Jacob, 945 N.Y.S.2d 863 (Sup. Ct. 2012) is distinguishable for similar reasons. There, the Complaint was filed on May 26, 2011, and the court's order requiring additional identification of trade secrets was issued on April 20, 2012, nearly a year after the case was filed and several months of discovery had taken place. *MSCI* also did not involve deletion and concealment of the misappropriated trade secrets by the defendants, preventing the plaintiff from specifically identifying what was taken. Finally, in *MSCI*, the only identification provided by the plaintiff after nearly one year of pending litigation was a "reference library" regarding its source code and did not provide any file specific information. *Id.* at *214. Here, by contrast, Moog has provided file names for each of the 136,994 files copied by Kim, over 62,000 hash values for those files, and a folder log for the over 1.3 million files copied by Pilkington.

Irth Sols., LLC v. Apex Data Sols. & Servs., LLC, No. 18-CV-6884-FPG, 2019 WL 283831 (W.D.N.Y. Jan. 22, 2019) is distinguishable on the facts. There, the plaintiff's "description of its trade secrets and its accusations of what Defendants copied from DigTrack focus on the various 'features' or 'modules' that are offered in the DigTrack program." *Id.* at *6. Yet, the fatal blow for the plaintiff was that it "admits that these 'features' or 'modules' are not trade secrets because they are publicly advertised on Plaintiff's own website, and because competitors in the industry offer these features as well." *Id.* This case is not similar, where Moog has expressly alleged that its trade secrets are not publicly advertised and are heavily secured. (Compl. ¶¶ 40-50). And, *Irth* involved adjudication of the plaintiff's motion for preliminary injunction whereas here, the parties are several months before the Preliminary Injunction hearing. Moog is entitled to complete initial discovery so that it can further specify the trade secrets stolen by Defendants during the Preliminary Injunction hearing.

Proofpoint, Inc. v. Vade Secure, Inc., No. 19-CV-04238-MMC, 2020 WL 836724 (N.D. Cal. Feb. 20, 2020), a California district court case, also involved adjudication of a preliminary injunction motion. The parties are months before that stage. And, notably, *Proofpoint* like all the other cases cited by Skyryse do not involve undisputed deletion and concealment of misappropriation preventing the plaintiff from identifying with precision what was taken.

Skyryse does not and cannot cite a case with procedural and factual similarities as this case where a court compelled further trade secret identification at the beginning stages of discovery and before any dispositive hearing took place.

6. Former Skyryse Employees Kim and Pilkington Are the Best Sources of What Was Misappropriated

The notion that Skyryse is “flying blind” in defending Moog’s trade secret claims are belied by the actual facts. Skyryse’s *own former employees* are the ones who know exactly what was copied and what has happened with Moog’s trade secrets. Indeed, Kim and Pilkington admit in their discovery responses that they retained possession of Moog Confidential Information (including source code) upon beginning employment at Skyryse. (Andoh Dec., Ex. H at RFA No. 2). Kim and Pilkington are also intimately familiar with Moog’s trade secrets given their work on Moog flight control programs for several years. Kim and Pilkington deleted evidence of their massive data copying and otherwise covered their tracks, giving Moog only limited information (which it has provided to Skyryse).

If Skyryse wants a more specific understanding of the nature and scope of Moog’s trade secrets, it merely needed to obtain information from Kim and Pilkington who remained employed with Skyryse for over a month and a half after this case was filed. And, the firing of Kim and Pilkington does not change the equation. Skyryse can depose Kim and Pilkington and ask whatever questions it wants regarding the data that was copied. Moog should not be punished

in providing information it does not presently have because Skyryse has now fired its two former employees who copied over 1.4 million files from Moog and covered their tracks.

B. Skyryse's Purported Burden and Volume Concerns are Unsubstantiated

1. Skyryse Consented to Expedited Discovery Regarding Moog's Trade Secrets

It is patently unfair for Skyryse to only now argue Moog has not sufficiently identified its trade secrets after it:

- ii. consented to expedited discovery specifically regarding Moog's trade secrets and non-public information nearly four months ago;
- iii. elected not to move to dismiss Skyryse's trade secret claim;
- iv. participated in written discovery specifically regarding Moog's trade secrets for months;
- v. produced thousands of documents to Moog, including Moog source code and other proprietary documents;
- vi. turned over 6 electronic devices and over 11,500 documents to iDS which all presumptively contain Moog non-public information under the March 11 Order.

If Skyryse had any genuine concerns about Moog's identification of trade secrets, it could have and should have formally moved on such objections at the outset of this case. It elected not to do so. It agreed to the March 11 Order having full notice of the allegations in the Complaint and Moog's trade secrets at issue. Skyryse claims it has preserved millions of documents, but has made very targeted productions to Moog and iDS of documents containing Moog non-public information. Skyryse cannot, on the one hand, claim it does not know a single trade secret at issue yet, on the other hand, participate in expedited discovery for several months and take several discovery actions based specifically on turning over Moog's trade secrets.

1. Skyryse Has Not Substantiated any Purported Burden

Skyryse complains that it has "been forced to respond to broad discovery requests regarding nearly the entirety of its business" and "sort through . . . over 30 million files and

more than seven terabytes of data.” (Mot. at pp. 15-16). Skyryse also contends Moog “has demanded virtually unlimited discovery into Skyryse’s business at extraordinary cost and disruption.” (*Id.* at p. 1). But, any burden or volume concerns presented by Skyryse are attributable to the conduct of its former employees.

Based on the limited information provided to date, it is undisputed that former Skyryse employees Kim and Pilkington copied over 1.4 million files upon leaving Moog and starting employment at Skyryse. Moog is aware of at least 43,000 source code files copied by Kim and Pilkington. Given the obfuscation by Kim and Pilkington, the volume of source code is likely much higher. The scope of misappropriation in this case is unique and staggering, and Skyryse must deal with the consequences. Skyryse cannot point to the finger at Moog.

Finally, Skyryse has not met its burden to substantiate its purported overbreadth issues. Skyryse has not provided any declaration, affidavit, or other admissible evidence substantiating its purported burden in responding to discovery in this case. This is Skyryse’s burden under the law. *See John Wiley & Sons, Inc. v. Book Dog Books, LLC*, 298 F.R.D. 184, 186 (S.D.N.Y. 2014) (party objecting on burden or overbreadth grounds must describe the burden by “submitting affidavits or offering evidence revealing the nature of the burden.”). Skyryse has also not substantiated any burden associated with producing its own source code and similar documents, including by describing the volume or number of lines of code that Skyryse has. Without any such evidence, Skyryse’s burden or overbreadth arguments fall flat.

C. Skyryse’s Requested Relief is Impracticable and Contrary to Law

Skyryse asks this Court to require “Moog to identify with particularity, every alleged trade secret it intends to assert in this action, including through a narrative response and not solely by invoking Rule 33(d).” (Mot. at p. 17). This request strains credibility.

1. Moog Has Properly Relied on Rule 33(d)

In response to Skyryse’s Interrogatory No. 1 asking Moog to identify its trade secrets at issue, Moog invoked Rule 33(d) and advised that documents responsive to this request (including source code) are available on the 9 electronic devices turned over by Moog to iDS. Skyryse has asked Moog to identify its source code, and Moog has properly done so by producing its source code under Rule 33(d). Courts acknowledge that a Rule 33(d) response is appropriate where the interrogatory asks for an identification of a large volume of source code. *Rensselaer Polytechnic Inst. v. Apple Inc.*, No. 1:13-CV-0633 DEP, 2014 WL 1871866, at *5 (N.D.N.Y. May 8, 2014) (where a party’s interrogatory sought “a full annotated narrative description of Siri’s source code,” the court determined that “that the appropriate vehicle for discerning the information sought is to make available, for plaintiffs’ review, Apple’s source code, which Apple has agreed to do” and that a Rule 33(d) response and production of source code in lieu of a narrative response “represents the most efficient and effective means of obtaining the information sought.”); *Kyocera Int’l, Inc. v. Nokia, Inc.*, No. 04 CV 1992 B (JFS), 2005 WL 8173284, at *5 (S.D. Cal. Aug. 9, 2005) (denying motion to compel further response where “pursuant to Rule 33(d), because [the requesting party] is now in possession of the source code, it appears that [the requesting party] is in a substantially similar position as [the producing party] in terms of ability to identify the requested information”). The exact same is true here where there are tens of thousands of source code files at issue. Moog has provided those files to iDS. Skyryse can inspect them and take depositions for further information.

Even so, Skyryse claims that Moog is required to at this early stage in the case give a narrative response identifying each and every trade secret at issue in the case, including every single line of non-public code. Notably, Skyryse cites to one Georgia district court case for the proposition that Rule 33(d) is improper in response to an interrogatory asking for identification

of trade secrets. *Lockheed Martin Corp. v. L-3 Commc'ns Corp.*, No. 1:05-CV-902-CAP, 2006 WL 8432941 (N.D. Ga. Oct. 27, 2006) is distinguishable for similar reasons as the other cases relied upon by Skyryse. In *Lockheed*, the court ordered the plaintiff to identify its trade secrets. However, this order was issued *after the case had been pending for 18 months*. *Id.* And, the court did not expressly state that a Rule 33(d) response is improper. Instead, it held: “To the extent that Lockheed supplements its response with documents, it must specify a page number or paragraph number referencing the precise material that it claims to be proprietary.” *Id.* at *2. Here, Moog cannot provide this granular specificity given the deletion of evidence and other obfuscation by Kim, Pilkington, and Skyryse.

Once Moog has had sufficient time to analyze the substantial evidence turned over to iDS, Moog is prepared to supplement its response to Skyryse’s Interrogatory No. 1, including by invoking Rule 33(d) as appropriate.

2. Moog is Not Required to Identify Each Line of Code That Constitutes Non-Public Information

Skyryse suggests that Moog, as part of a narrative response, must identify “which specific lines or blocks of its source code . . . it alleges to be trade secrets.” (Mot. at p. 13). Not only is such a request impracticable and improper for the reasons set forth above, but it is also legally deficient.

It is well-settled that although “matters of public knowledge or of general knowledge in an industry cannot be categorized as trade secrets, a compilation of the public information which incorporates the information in a unique way is, nonetheless, protectable as a trade secret.” *See Integ. Cash Mgmt. Servs., Inc. v. Digital Trans., Inc.*, 920 F.2d 171, 174 (2d Cir.1990). A “trade secret may consist of a compilation of data, public sources or a combination of proprietary and public sources.” *United States v. Nosal*, 844 F.3d 1024, 1042-43 (9th Cir. 2016); *Norbrook*

Lab'ys Ltd. v. G.C. Hanford Mfg. Co., 297 F. Supp. 2d 463, 483 (N.D.N.Y. 2003), *aff'd*, 126 F. App'x 507 (2d Cir. 2005) (“A trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process, design and operation of which, in unique combination, affords a competitive advantage and is a protectable secret.”) (internal citations omitted); *Harbor Software, Inc. v. Applied Sys., Inc.*, 887 F. Supp. 86, 90 (S.D.N.Y. 1995) (“Case law supports the proposition that the overall design of a software program may be protectable as a trade secret, even if the individual components of that program are common knowledge in the programming industry.”).

The fact that there may be lines of code that are public knowledge or do not specifically constitute Moog non-public information (which Moog does not concede) does not make it so that only certain portions of Moog’s flight control source code are protectable trade secrets and must be specifically identified. Indeed, Moog has spent over 15 years of research and development efforts, and invested well over \$100 million dollars, to compile and build its flight control programs including its source code. (ECF 1, ¶¶ 27-39). It is extremely common for protectable trade secrets to include public information (such as customer lists), but it is often the time, effort, and resources used to compile such information (along with other non-public information) that warrants trade secret protection. For this additional reason, Skyrise’s request that Moog specifically identify in a narrative response each line of code that constitutes a trade secret is improper and should be denied.

IV. CONCLUSION

Moog respectfully requests that the Court deny Skyrise's Motion in its entirety.

Dated: New York, New York
July 5, 2022

SHEPPARD, MULLIN, RICHTER & HAMPTON LLP

By: /s/ Rena Andoh
Rena Andoh
Travis J. Anderson (*pro hac vice*)
Tyler E. Baker (*pro hac vice*)
Kazim A. Naqvi (*pro hac vice*)
30 Rockefeller Plaza
New York, New York 10112
Telephone: (212) 653-8700

and

HODGSON RUSS LLP

By: /s/ Robert J. Fluskey, Jr.
Robert J. Fluskey, Jr.
Melissa N. Subjeck
Pauline T. Muto
The Guaranty Building
140 Pearl Street, Suite 100
Buffalo, New York 14202
(716) 856-4000
Attorneys for Plaintiff Moog Inc.